대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2003년 제 0080752 호
Application Number 10-2003-0080752

출 원 년 월 일 : 2003년 11월 14일
Date of Application NOV 14, 2003

출 원 인 : 주식회사 넷츠
Applicant(s) NETS CO., LTD.

2004 년 11 월 30 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【관리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【출원일자】	2003.11.14
【발명의 명칭】	엑스트라넷 액세스제어 장치 및 방법
【발명의 영문명칭】	Extranet access management apparatus and method
【출원인】	
【명칭】	주식회사 넷츠
【출원인코드】	1-2000-040398-5
【대리인】	
【성명】	박승민
【대리인코드】	9-1999-000248-5
【포괄위임등록번호】	2000-049103-0
【발명자】	
【성명의 국문표기】	이세현
【성명의 영문표기】	LEE,Se Hyun
【주민등록번호】	730915-1674621
【우편번호】	138-916
【주소】	서울특별시 송파구 잠실동 잠실주공아파트 5단지 508-1004
【국적】	KR
【발명자】	
【성명의 국문표기】	류영준
【성명의 영문표기】	RYU,Young Jun
【주민등록번호】	770604-1019018
【우편번호】	135-874
【주소】	서울특별시 강남구 삼성2동 112~13 804호
【국적】	KR
【발명자】	
【성명의 국문표기】	문성광
【성명의 영문표기】	MOON,Sung Kwang
【주민등록번호】	731011-1183011

【우편번호】	151-762
【주소】	서울특별시 관악구 봉천2동 동아아파트 201-1912
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 박승민 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	2 면 2,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	4 항 237,000 원
【합계】	268,000 원
【감면사유】	중소기업
【감면후 수수료】	134,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통 2.중소기업기본법시행령 제2조에의한 중소기업에 해당함을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 액세스제어 장치 및 방법에 관한 것으로, 보다 구체적으로는, xSP를 한 엑스트라넷에서의 액세스를 제어하는 장치 및 방법(이하, "본 발명의 액세스제 장치 및 방법"이라 함)에 관한 것이다. 본 발명에 따르면, 권한의 중앙집중으로 한 문제점 및 권한캐시 문제를 해결하기 위하여 ACL캐시를 이용하여 액세스제어의 한을 분산하고, AA 서버(인증서버)를 이용하여 분산된 액세스제어 역할을 동기화하다. 또한, 유저 웹브라우저 쿠키를 이용한 인증/권한 관리를 적용하여 세션관리의 효율성을 해결하였고, 인터넷 보안 표준 지원 및 다양한 보안/암호화기술 및 유저의 액세스제어 처리 등의 추가기능을 부여하였다.

【표도】

도 2

【인어】

스제어, 접근제어, 엑스트라넷, xSP, 캐시, 쿠키

【명세서】

【발명의 명칭】

엑스트라넷 액세스제어 장치 및 방법{Extranet access management apparatus and
hod}

【도면의 간단한 설명】

도1은 본 발명에 따른 액세스제어 장치의 전체적인 시스템 개략구성도.

도2는 본 발명에 따른 장치의 구체적 구성도.

도3a 및 도3b는 인증시의 권한설정 절차를 나타내는 도면.

도4a 및 도4b는 권한조회 절차를 나타내는 도면.

도5aa, 5ab, 5b는 권한변경 절차를 나타내는 도면.

도6aa, 6ab, 6ba, 6bb는 ACL캐시 동기화 절차를 나타내는 도면.

도7은 ACL캐시를 이용한 액세스제어 역할의 분산 개념을 나타내는 도면.

도8은 AA서버를 이용한 분산된 액세스제어 역할의 동기화 개념을 나타내는
면.

도9는 유저 웹브라우저 쿠키를 이용한 인증/권한 관리 개념을 나타내는 도면.

발명의 상세한 설명】

발명의 목적】

발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 액세스제어 장치 및 방법에 관한 것으로, 보다 구체적으로는, xSP급 한 엑스트라넷에서의 액세스를 제어하는 장치 및 방법(이하, "본 발명의 액세스제 장치 및 방법"이라 함)에 관한 것이다.

종래 xSP(extended service provider)에서의 유저관리 방식은 단순 인증 방식에 |반을 두고 있다. 그러나, 온라인 시장의 포화에 따라서 새로운 시장 개척이 필요 게 되었다. 특히, 역할별, 리소스별로 액세스를 제어할 필요성이 커지고 있다.

기존에 유통되고 있는 액세스제어 솔루션 또는 패키지는 소규모 포털사이트나 내 인트라넷을 대상으로 하고 있다. 이들은 실시간 중앙집중식 권한관리를 하고 있며 제한된 유저가 이용하며 복잡한 계층구조를 갖고 있어서, 비용이 높은 반면에 율이 낮은 단점이 있다.

보다 구체적으로 종래의 액세스 제어 방식의 문제점을 살펴본다.

1. 권한의 중앙집중 관리에 따른 과도한 네트웍 트래픽

웹서버와 디렉토리(또는 DB) 서버 사이에 위치한 중앙 관리서버가 실시간으로 션관리 및 액세스제어를 담당한다. 그리고 웹서버로 오는 모든 유저의 요청에 대하 검사/권한을 부여한다. 따라서, 유저의 수가 적고 비교적 네트웍 사용량이 적은 내 인트라넷 또는 소규모 회원제 포털사이트에 적합한 모델이다. 또한, xSP의 특성 000만 이상의 유저수, 단순한 계층 구조, 빈번한 네트웍 사용량)을 고려할 때 중앙

중 관리 모델은 대규모 네트워 트래픽으로 인한 성능저하와 이의 해결을 위한 과도 비용(장비 및 유지보수)이 요구된다.

2. 권한캐시의 불안정성

종래에, 중앙집중 관리에 따른 단점을 극복하기 위해 "권한캐시"를 두고 있다. 는, 동일한 리소스나 유저의 요청에 의해 해당 웹서버에서 직접 처리함으로써 네트 트래픽을 줄여 처리성능을 개선하는 방법을 제공하는 것이나, 캐시의 간소화가 불능하고 안정적인 서비스를 위한 적정 캐시 크기조절이 어려워 오랜 기간의 시행착가 불가피하다.

3. 세션관리의 비효율성

모든 유저의 세션을 중앙서버에서 관리하고 있으므로, 소규모 인트라넷 모델에 적합할 뿐이다. 실시간 세션관리를 위해 kB 단위 이상의 큰 쿠키를 유지해야 하지 . xSP의 특성상 중앙집중 세션관리와 과도한 쿠키 크기는 네트웍 부하나 서버 가용의 측면에서 대단히 비효율적이다.

발명이 이루고자 하는 기술적 과제】

이에, 대규모이면서도 고성능의 요건을 만족하는 새로운 액세스제어 솔루션이 요해진다. 따라서, 본 발명은 대규모 포털사이트에 적합한 고성능의 인증 및 액세 제어 장치 및 방법을 제공함을 목적으로 한다.

발명의 구성 및 작용】

본 명세서에서 사용된 기본적인 용어를 다음과 같이 정의한다.

- ACE(access control entry) - 특정 웹서버의 리소스에 액세스한 수 있는 각 세스제어 항목으로서, ID, 이름, 소속사이트 도메인, 서버목록, 리소스 목록, 변경리 URL, 설명 등의 항목으로 구성된다.

- ACL(access control list) - ACE들의 목록(집합)

- ACL 캐시 - 도메인웹서버에서 ACL을 저장하고 있는 어플리케이션 수(메모리) 공간

- Role - 유저가 액세스 가능한 ACE들의 집합으로서, 유저스키마(scheme)의 권 속성을 이용하여 유저 Role을 정의한 수 있다. Role 정보는 ACE가 많아질수록 쿠키 저장되는 정보량이 증가하게 되므로, Role 정보의 축소방안이 필요해진다. Role을 CE ID 목록으로 저장할 경우에, ACE 목록을 사람이 알수 있는 이름(human readable me)으로 지정시에는 정보량이 매우 증가하게 된다. 따라서, ACE ID를 일련의 -zA-Z0-9]의 62진수 문자열로 표현하면, 정보량이 작아질 수 있다. 즉, 2자리일 경 에는 3,844개의 Role 정보 표현이 가능하며, 3자리일 경우에는 238,328개의 Role 보 표현이 가능해진다(예를 들어, Role = A0:B2:cZ:Ku:Z3:...와 같이 표현한다). le은 유저 인증시 AA쿠키에 저장된다.

- 유저스키마(scheme) - ID, 비밀번호 등의 여러가지 유저 속성이 정의된 저장 조.

- AA(authentication and authorization)서버 - 유저 인증 및 Role 설정, 도메 웹서버의 ACL캐시 동기화를 담당

- AA 쿠키 - 유저의 인증 및 권한정보를 포함하고 있는 쿠키

<본 발명의 개요>

본 발명에 따르면, 권한의 중앙집중으로 인한 문제점 및 권한캐시 문제를 해결기 위하여 ACL캐시를 이용하여 액세스제어의 역할을 분산하고, AA 서버(인증서버) 이용하여 분산된 액세스제어 역할을 동기화하였다. 또한, 유저 웹브라우저 쿠키를 용한 인증/권한 관리를 적용하여 세션관리의 비효율성을 해결하였고, 인터넷 보안 준 지원 및 다양한 보안/암호화기술 및 유저정의 액세스제어 처리 등의 추가기능을 여하였다.

도1은 본 발명의 액세스제어 장치의 시스템 구성도를 간략하게 나타낸다. 다수 유저가 가입되어 있는 도메인웹서버(100a, 100b, ...)에서 도메인별로 ACL 정보를 l용하여 권한 검사를 수행한다. 그 결과 도메인웹서버(100a, 100b, ...)에서 암호된 Role정보 쿠키를 출력하면, 이 쿠키 신호는 부하분배 및 오류수정 모듈 00)(load-balancing/fault-tolerance module)을 거쳐 AA 서버(300)에서 인증되고 한이 부여되어 권한정보 저장 모듈(400)에 Role, ACL, ACE 정보가 저장된다.

본 발명에 따른 액세스제어 장치의 기술적 특징을 미리 정리해 보면 다음과 같 .

- ACL캐시를 이용한 액세스제어 역할의 분산 (도7 참조)

종래의 전통적인 캐시기법(한 번 요청된 리소스에 대한 권한을 캐시로 저장)은 효율적이었는바, ACL을 단순화(기호화)하여 통째로 ACL 캐시로 저장함으로써, 액세 제어 역할을 각 도메인웹서버(100)에 맡김으로써 액세스제어를 위한 서버간 네트웍

트래픽을 최소화하였다. 즉, 각 도메인웹서버(100)에서 ACL 캐시를 관리하고 자체적로 액세스제어 처리를 수행한다.

- AA서버를 이용한 분산된 액세스제어 역할의 등기화 (도8 참조)

위와 같이 액세스제어 역할이 분리됨에 따라, 서버간 ACL캐시의 자동 동기화가 요해진다. 이를 위해, 도8에서와 같이, 웹서버(100)의 최초 구동시에 AA서버(300)부터 ACL캐시를 초기화하고, AA 서버(300)에서 관리자에 의해 ACL이 변경된 경우에 실시간으로 해당 웹서버(100)의 ACL캐시 정보를 갱신하여 등기화를 유지한다. 또, AA서버(300)은 ACL 등기화 로그를 관리함으로써 장애 및 유지보수를 용이하게 한다.

- 유저 웹브라우저 쿠키를 이용한 인증/권한 관리 (도9 참조)

대규모 유저의 세션을 서버에서 관리하는 것은 부적절하다. 따라서 암호화된 유저 웹브라우저 쿠키를 통해 유저의 세션을 관리함으로써 서버 부하를 최소화하고 있다. 이렇게 쿠키와 표준 HTTP 프로토콜을 이용한 고속 인증 처리를 수행하고, 인증시는 단순화(기호화)시킨 Role을 쿠키로 저장/관리하므로써, 도메인웹서버(100)의 ACL캐시와 쿠키의 Role을 이용한 액세스 제어를 행하고 있다.

<본 발명의 장치의 구성>

이제, 본 발명의 액세스제어 장치의 구체적인 구성 및 작용에 대해서 설명한다. 도2는 도1에 나타낸 구성 중에서 본 발명의 액세스제어 장치에 고유한 구성만을 구체적으로 도시한 것이다. 도메인웹서버(100)와, AA서버(300)와, 권한정보 저장모듈

00)이 상호 연결되어 있고, 유저 웹브라우저(500)는 AA서버(300) 및 도메인웹서버 00)과 HTTP 방식으로 연결되어 있다.

도2에서, AA서버(300)는, 인증(authentication) 및 권한부여(authorization)를 당하는 AA(인증/권한)모듈(302)과, 본 발명의 액세스제어 장치의 관리를 담당하고 한정책을 관리하는 관리모듈(304)과, AA서버(300)와 각 도메인웹서버(100)등의 ACL 시를 동기화하는 ACL캐시 제어모듈(306)과, 유저에게 설정해 줄 AA쿠키를 암호화하 암호화모듈(308)과, 권한정보 저장모듈(400)에 독립적인 시스템 운영을 제공하는 키마프로바이더(310) 및 유저프로바이더(312)로 구성된다.

다음에, 도메인웹서버(100)는, ACL캐시를 이용하여 유저의 액세스 여부간 판별 는 AA모듈(102)과, AA서버(300)로부터 전달되어온 ACL캐시(104)와, 암호화된 AA쿠 를 해독하는 복호화모듈(106)과, 유저 웹브라우저(500)로부터의 리소스요청을 처리 는 모듈(108)로 구성된다.

도7-9를 통해 앞에서 설명한 것과 같이, 유저 웹브라우저(500)과 AA서버(300) 도메인웹서버(100) 사이의 요청/응답(request/response)은 AA쿠키에 의해 이루어 다.

이상과 같이 구성되는 본 발명의 액세스제어 장치의 작용에 대해서 차례로 설명 다. 본 발명에 따른 액세스제어 장치의 작용은 액세스제어를 수행하는 방법상의 절 와 본질적으로 같은 것이므로 도2의 액세스제어 장치의 작용은 본 발명의 액세스제 방법과 함께 설명한다.

우선, 도3a는 인증시의 권한설정 절차를 나타내는 도면이다. 유저가 인터넷을 해 도메인웹서버(100)에 로그인하면 도메인웹서버(100)에서는 AA서버(300)에 인증 청을 하고, AA서버(300)는 유저 ID와 패스워드를 이용하여 권한정보(400)에 인증속 및 유저권한 속성을 조회한다. 조회결과, AA서버(300)는 유저 브라우저에 AA쿠키 Role값을 설정한다(예를 들어, Role=A0:K1:z8:03).

도3a에서 설명한 권한설정의 기능적 처리흐름을 도2의 구성도로써 표시하면 도와 같이 나타낼 수 있다. 순서대로 설명하면, 유저 웹브라우저(500)에서 도메인웹버(100)에 접속하면[S1] 도메인웹서버(100)의 AA모듈(102)에서는 인증확인을 해서 TP를 통해 다시 유저 웹브라우저(500)로 보내고[S2] AA서버(300)의 AA모듈(302)에 증요청을 한다[S3]. AA서버(300)의 AA모듈(302)은 스키마프로바이더(310)에 인증조를 하고[S4] 스키마프로바이더(310)에서는 권한정보 저장모듈(400)로부터 사이트조를 하고[S5] 그 결과를 유저프로바이더(312)로 전달한다. 유저프로바이더(312)에서 권한정보 저장모듈(400)에 유저 권한 조회를 하여[S6] 인증 및 권한 설정을 해서 저 웹브라우저(500)에 전송한다[S7].

다음은, 권한 조회에 대하여 설명한다. 우선, ACL캐시에 있어서, 각 도메인웹서는 자신과 관련된 ACL을 캐시로 유지한다. 그리고, 유저의 Role에서 각 ACE의 리소 문자열을 조회한다. 그리고, ACE의 리소스 항목에 대한 문자열 패턴검색을 통하여 턴을 검색한다. 권한 조회에 대해서 도4a 및 도4b를 참조하여 구체적으로 설명한

.

도4a에서, 우선 유저가 도메인웹서버(100)에 페이지(URL) 액세스요청을 하면, 쿠키에서 Role을 추출한다(예컨대, Role=A8:Bf:03). 도메인웹서버(100)에서는 유저

한 검사를 수행하는데, 우선, 요청된 액세스리소스의 ACE ID를 ACL캐시에서 추출하 액세스리소스의 ACE ID가 유저 Role에 존재하는지 조회한다. 조회 결과, 유저 le에 ACE ID가 있을 경우에는 액세스권한을 부여한다.

도4b를 통해 그 기능적 흐름을 설명한다. 도4b에서 유저가 도메인웹서버(100)에 세스(access)하면[S1] 도메인웹서버(100)의 AA모듈(102)에서는 권한검사를 하고 2] 리소스요청 처리모듈(108)은 권한조회 요청을 처리하고[S3] 그 결과를 유저 웹 라우저에 보내어 응답한다[S4].

다음, 유저 권한변경에 대하여 설명한다. 도5aa는 서비스가입을 하는 경우의 흐 개요도이고, 도5ab는 서비스탈퇴를 하는 경우의 흐름 개요도이다. 도5aa에서 유저 서비스 가입을 요청하면 도메인웹서버에서는 유저ID와 Role코드를 AA서버에 전송 고, AA서버는 유저 속성에 Role코드를 추가한다. 반대로 유저가 서비스 탈퇴를 요 하면 도메인웹서버에서는 유저ID와 Role코드를 AA서버에 전송하고, AA서버는 유저 성에서 Role코드를 삭제한다.

이상의 처리흐름을 도2의 구성도로써 설명하면 도5b와 같다. 유저웹브라우저에 서비스가입 또는 탈퇴를 요청하면[S1], 도메인웹서버(100)의 리소스요청 리모듈(108)에서는 AA서버의 AA모듈(302)에 가입/탈퇴요청을 하고[S2], AA모듈 02)은 유저 권한정보를 수정하여 유저프로바이더(312)에 전송하고[S3], 유저프로바 더(312)는 수정된 정보를 권한정보 저장모듈(400)에 보내어 유저정보를 업데이트한 [S4]. 이때 AA모듈(302)은 유저정보가 변경되었음을 도메인웹서버의 리소스요청 처 모듈(108)에 보고하여[S5] 유저에게 가입/탈퇴가 완료되었음을 알리도록 한다[S6].

한편, 본 발명에서 필수적인 ACL캐시의 등기화에 대해서는 다음과 같이 구체적로 설명할 수 있다. ACL캐시는 각 도메인웹서버가 유저의 액세스 요청시에 Role을 회하기 위해 필요한 것으로서, 도메인웹서버는 조회를 위하여 AA서버와 추가적으로 신하는 것을 피하기 위해 자체 ACL캐시를 유지하고 있다. 캐시는 어플리케이션 변(어플리케이션을 사용하는 모든 클라이언트가 공유하는 변수)로서 웹서버의 메모리에 상주하고 있는 메모리이다.

이 ACL캐시를 각 도메인웹서버에서 보관하고 있다. 따라서 AA서버에서 ACL을 변할 때에 도메인웹서버들과의 ACL캐시의 등기화문제가 발생한다. 이 문제는 도6aa-6bb와 같은 처리로 해결한다.

도6aa는 초기화 절차를 나타내는 것으로서, 도메인웹서버를 가동할 때마다 AA서로부터 ACL캐시를 초기화한다. 즉, 도메인웹서버가 가동하면 AA서버에 ACL캐시를 청하고, AA서버에서는 최신 ACL을 권한정보 저장모듈에서 조회하여 도메인웹서버에 달하여 응답한다. 도6ab는 상기 절차를 도2의 구성도로써 설명하기 위한 것으로서, 메인웹서버(100)의 AA모듈(102)이 AA서버의 ACL캐시 제어모듈(306)에 캐시요청을 면[S1], ACL캐시 제어모듈(306)은 권한정보 저장모듈(400)로부터 ACL캐시를 조회하[S2] 다시 도메인웹서버(100)의 AA모듈(102)로 전달한다[S3].

도6ba는 초기화 후 ACL캐시의 등기화를 나타내는 절차도이다. ACL이 추가, 제, 변경될 경우 해당 도메인 웹서버로 갱신 정보를 전송하면, 해당 도메인웹서버서는 실시간으로 캐시정보를 업데이트한다. 한 번의 업데이트가 실패하더라도 주기으로 캐시를 갱신하기 때문에 최신정보는 항상 유지가 가능하다. 도6ba에서 볼 때, 트라넷을 통해 관리자가 ACL관리를 선택하면 AA서버에서는 ACL캐시를 업데이트할

메인웹서버를 선택하여 해당 도메인웹서버에 ACL캐시 갱신을 요청하고(요청시에는 E의 세부정보가 포함된다), 해당 도메인웹서버에서는 요청받은 ACL정보를 신한다. 도6bb는 상기 절차를 도2의 구성도로써 설명하기 위한 것으로서, 관리자가 서버의 ACL캐시 제어모듈(306)로 하여금 권한변경을 명령하면[S1], ACL캐시 제어모(306)은 정보권한 저장모듈(400)에 ACL변경을 요청하고 도메인웹서버의 ACL캐시 04)에 캐시동기화를 명령한다.

여기서, 관리자는 ACE관리(ACE의 추가/삭제, ACE 소속 사이트/유저/ACE ID/ACE 름으로의 검색) 및 편집, 유저 Role 관리 등을 수행하는 모듈이다.

발명의 효과】

이상에서와 같이 본 발명에 따르면, 종래의 액세스 제어 방식의 문제점, 즉, 1) 한의 중앙집중 관리에 따른 과도한 네트웍 트래픽, 2) 권한캐시의 불안정성, 3) 세 관리의 비효율성 등의 문제점을 해결할 수 있다. 본 발명은 특히, xSP용 엑스트라 에서의 액세스 콘트롤에 적용시에 그 효용성이 크다.

【특허청구범위】

【청구항 1】

다수의 도메인웹서버와, 각 도메인웹서버로의 액세스 인증 및 권한관리를 담당하는 AA서버와, 권한정보을 저장하는 모듈과, 상기 AA서버 및 도메인웹서버와 연결되는 유저 웹브라우저로 구성되는 시스템에 있어서,

상기 AA서버는 인증(authentication) 및 권한부여(authorization)를 담당하는 모듈과, AA서버와 각 도메인웹서버들의 ACL캐시를 동기화하는 ACL캐시 제어모듈과, 저에게 설정해 준 AA쿠키를 암호화하는 암호화모듈과, 권한정보 저장모듈에 독립적 시스템 운영을 제공하는 스키마프로바이더 및 유저프로바이더로 구성되고,

상기 도메인웹서버는 ACL캐시를 이용하여 유저의 액세스 여부를 판별하는 AA모과, AA서버로부터 전달되어온 ACL캐시 모듈과, 암호화된 AA쿠키를 해독하는 복호화듈과, 유저 웹브라우저로부터의 리소스요청을 처리하는 모듈로 구성되어,

다수의 유저가 가입되어 있는 도메인웹서버에서 도메인별로 ACL 정보를 이용하 권한 검사를 수행하면, 그 결과 도메인웹서버에서 암호화된 Role정보 쿠키를 출력고, 이 쿠키 신호는 AA 서버에서 인증되고 권한이 부여되어 권한정보 저장 모듈에le, ACL, ACE 정보가 저장되는 것을 특징으로 하는, 엑스트라넷 액세스제어 장치.

【청구항 2】

제1항과 같이 구성되는 장치에 의해 이루어지는 액세스제어 방법으로서,

유저 웹브라우저에서 도메인웹서버에 접속하는 단계, 도메인웹서버의 AA모듈에 인증확인을 해서 HTTP를 통해 다시 유저 웹브라우저로 보내는 단계, AA서버의 AA

듈에 인증요청을 하면, AA서버의 AA모듈은 스키마프로바이더에 인증조회를 하고 스마프로바이더에서는 권한정보 저장모듈로부터 사이트조회를 하여 그 결과를 유저프바이더로 전달하는 단계, 유저프로바이더에서는 권한정보 저장모듈에 유저 권한 조를 하여 인증 및 권한 설정을 해서 유저 웹브라우저에 전송하는 단계를 포함하는 증시의 권한설정 절차와.

유저가 도메인웹서버에 액세스하면 도메인웹서버의 AA모듈에서는 권한검사를 하 리소스요청 처리모듈은 권한조회 요청을 처리하고 그 결과를 유저 웹브라우저에 내어 응답하는 단계를 포함하는 권한 조회 절차를 포함하는, 엑스트라넷 액세스제 방법.

청구항 3]

제2항에 있어서,

유저웹브라우저에서 서비스가입 또는 탈퇴를 요청하면, 도메인웹서버(100)의 리스요청 처리모듈에서는 AA서버의 AA모듈에 가입/탈퇴요청을 하고, AA모듈은 유저 한정보를 수정하여 유저프로바이더에 전송하고, 유저프로바이더는 수정된 정보를 한정보 저장모듈에 보내어 유저정보를 업데이트하는 단계와, AA모듈은 유저정보가 경되었음을 도메인웹서버의 리소스요청 처리모듈에 보고하여 유저에게 가입/탈퇴가 료되었음을 알리는 단계를 포함하는 유저 권한변경 절차를 추가로 포함하는, 엑스라넷 액세스제어 방법.

청구항 4]

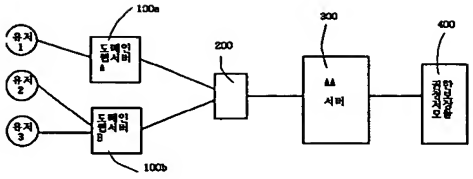
제2항에 있어서,

도메인웹서버의 AA모듈이 AA서버의 ACL캐시 제어모듈에 캐시요청을 하면, ACL 시 제어모듈은 권한정보 저장모듈로부터 ACL캐시를 조회하여 다시 도메인웹서버의 모듈로 전달하는 ACL 초기화 단계와,

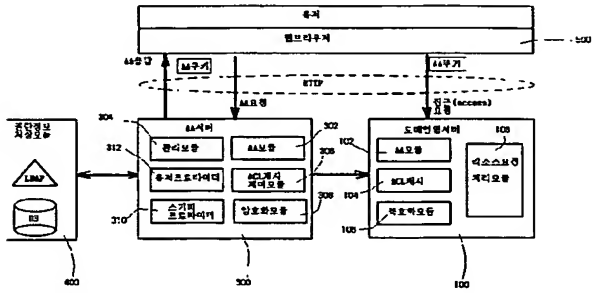
관리자가 AA서버의 ACL캐시 제어모듈로 하여금 권한변경을 명령하면, ACL캐시 어모듈은 정보권한 저장모듈에 ACL변경을 요청하고 도메인웹서버의 ACL캐시에 캐시 기화를 명령하는 ACL 등기화 단계가 추가로 포함되는, 엑스트라넷 액세스제어 법.

【도면】

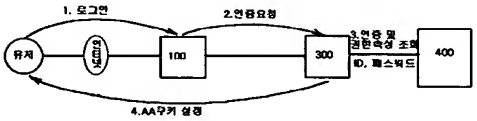
【도 1】


유저 1
유저 2
유저 3
도메인 웹서버 A
도메인 웹서버 B
100a
100b
200
300
AA 서버
400

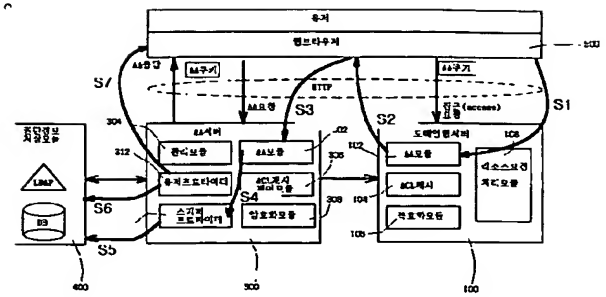
【도 2】


유저
웹브라우저
AA쿠키
HTTP
AA요청
접근(access) 요청
AA서버
관리모듈
AA모듈
유저프로파일러
ACL갱신 제어모듈
스키마 프로파일러
암호화모듈
도메인웹서버
AA모듈
ACL캐시
악호학모듈
리소스보호 제어모듈
LDAP
DB
304
312
310
302
306
308
102
104
106
108
400
300
100

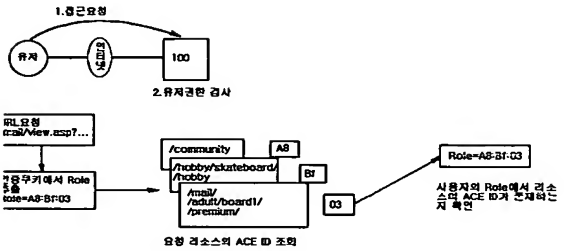
【도 3a】


1. 로그인
2.인증요청
유저
100
300
400
4.AA쿠키 설정

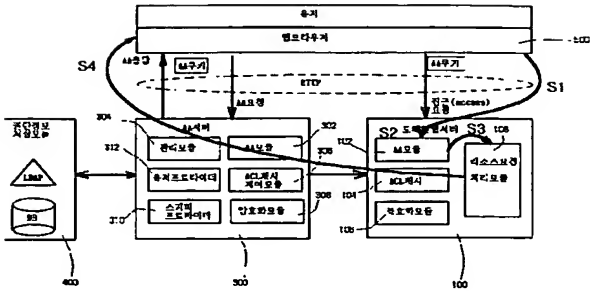
도 3b]


S1
S2
S3
S4
S5
S6
S7
HTTP
100
200
300
400

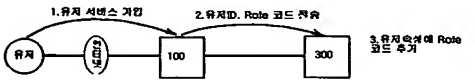
도 4a]


1.접근요청
유저
100
2.유저권한 검사
/community
/hobby/skateboard/
/hobby
/mail/
/adult/board1/
/premium/
A8
B1
03
Role=A8:B1:03
사용자의 Role에서 리소스의 ACE ID가 존재하는지 확인
요청 리소스의 ACE ID 조회

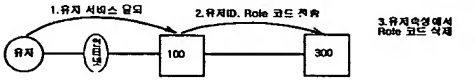
【도 4b】



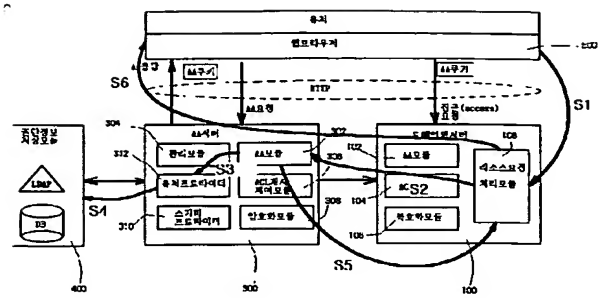
【도 5aa】



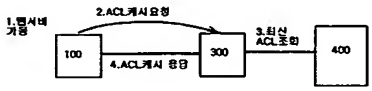
【도 5ab】



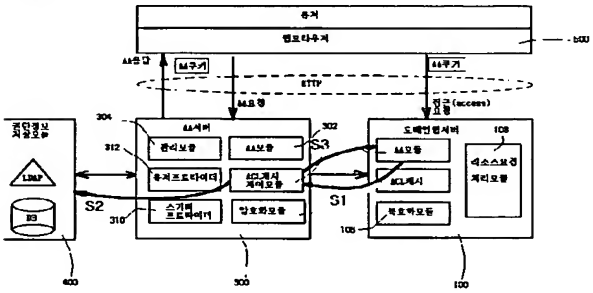
[도 5b]



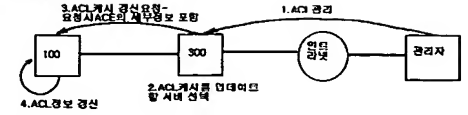
[도 6aa]



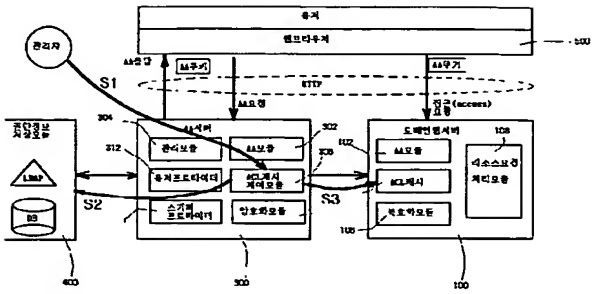
[도 6ab]



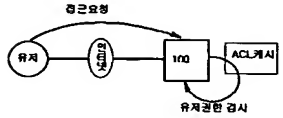
도 6ba]



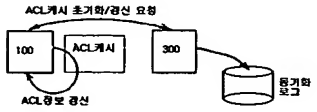
도 6bb]



도 7]



도 8]



근 9)